Chapter 6

The Duty to Provide Information to the Data Subject: Articles 10 and 11 of Directive 95/46/EC

Deryck Beyleveld*

Introduction

According to Article 10 of Directive 95/46/EC, which applies 'in cases of collection of data from the data subject';

> Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
>
> (a) the identity of the controller and of his representative, if any;
> (b) the purpose of the processing for which the data are intended;
> (c) any further information such as:
>
> - the recipients or categories of recipients of the data,
> - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
> - the existence of the right of access and the right to rectify the data concerning him,
>
> in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

According to Article 11(1),

> *Where the data have not been obtained from the data subject* [my emphasis], Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except when he already has it:

---

* Professor of Jurisprudence, Faculty of Law, University of Sheffield, Director of the Sheffield Institute of Biotechnological Law and Ethics (SIBLE), Co-ordinator of PRIVIREAL.

(a) the identity of the controller and of his representative, if any;
(b) the purpose of the processing;
(c) any further information such as
    - the categories of data concerned,
    - the recipients or categories of recipients,
    - the existence of the right of access and the right to rectify the data concerning him,

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

That the provision of 'further information' referred to in Articles 10 and 11(1) (both specified and unspecified) is for the purpose of fair processing links these provisions to the principle of data protection laid down in Article 6(1)(a), according to which 'Member States shall provide that personal data must be . . . processed fairly and lawfully'.[1]

This linkage is entirely appropriate, because the provision of information to the data subject prescribed by Articles 10 and 11(1) is of central importance to the objective of the Directive, which is to ensure an adequate level of protection of fundamental rights and freedoms (in particular, the right to privacy) of natural persons with respect to the processing of personal data in all Member States. This is in order that Member States should have no legitimate excuse to restrict or prohibit the free flow of personal data between themselves on the grounds that other Member States do not provide adequate protection for fundamental rights and freedoms (see Article 1 and Recitals 1 to 10, especially Recitals 7 to 10).

The right to privacy referred to here is, of course, that provided by Article 8 of the European Convention on Human Rights (ECHR) as a fundamental principle of EC law (see Recital 10). In line with this right, the Directive:

1. prohibits the processing of sensitive personal data (Article 8(1)), unless certain conditions are satisfied (Articles 8(2)–(7)), which, in principle, reflect (*inter alia*) the need for a justification to be provided for a breach of privacy in the terms of Article 8(2) ECHR.[2] Although the explicit consent of the data subject is only one of the conditions provided by Article 8(2)–(7) of the Directive for the lifting of the prohibition of Article 8(1) of the Directive, it seems to me that this implies (at least in the case of sensitive personal data) that explicit consent must be obtained unless a justification for not doing so exists in the terms of Article 8(2) ECHR;[3]

---

[1] See also Recital 38, which states that the provision of all the Article 10 and 11(1 information is necessary for processing to be fair.

[2] Because the Directive aims to protect fundamental rights and freedoms generally (se Article 1(1)), and not merely privacy, not only Article 8 ECHR is relevant.

[3] This is because the European Court of Human Rights has held in *M.S v. Sweden* [1997] 2 *EHRR* 313, paragraphs 34–35 that to process/disclose sensitive personal data without th subject's consent (even where the information is processed/disclosed to persons acting und

2. provides the data subject with a right:
   - to find out from the data controller about whether or not personal data relating to him or her is being processed, for which purposes, and to whom it is being disclosed, and about the source of this data (see Article 12(a));
   - to be told of the logic behind any automatic processing of such data (see Article 12(a));
   - to secure the rectification, erasure or blocking of processing that does not comply with the provisions of the Directive (see Article 12(b));
   - to object on compelling legitimate grounds to the processing of personal data relating to the data subject (see Article 14(a));
   - to object to the use of personal data relating to the data subject being used for purposes of direct marketing (see Article 14(b)); and
   - not to be subject to any decision that significantly affects the data subject that is based solely on automatic processing of personal data relating to the data subject (see Article 15(1)).

Bearing in mind that Article 2(h) defines 'consent' as 'any freely given specific and informed indication' by which the data subject signifies agreement, possession of the information required to be provided by Articles 10 and 11(1) is clearly necessary for the data subject to give a valid consent. Equally, possession of this information is necessary for the data subject to be able to exercise the rights provided by Articles 12, 14 and 15 of the Directive. Thus, to withhold Articles 10 and 11(1) information from the data subject, is to interfere with the rights of the data subject provided by Articles 12, 14 and 15 and with his or her right to privacy in so far as this requires the data subject to be granted the right to consent to the use of his or her personal data.

In essence, logic and fairness both demand that if a right is granted to someone ('Y') to something ('X') then Y must be granted a right to any necessary means to X as well. For this reason, a right to the provision of the information prescribed or indicated in Articles 10 and 11(1) is implied by Articles 7, 8, 12, 14 and 15. While the Directive does not explicitly present the provision of the Article 10 and Article 11(1) information as a right of the data subject, but as a duty of the data controller, because of the general correlativity of claim rights of a person with duties of others, to present this information provision as a duty of the controller is not incompatible with it being a right of the data subject. However, to present it as a duty of the data controller is appropriate, simply because whether or not the data subject will obtain any knowledge of relevant processing will be very much in the hands of others, especially, the data controller.

---

a duty of confidence) is an interference with the right provided by Article 8(1) ECHR (even though the Court went on to say that in the circumstances of the case the interference was justified under Article 8(2) ECHR). Under Article 8(2) ECHR, a breach of Article 8(1) can only be justified if necessary and proportionate for the legitimate purposes laid down in Article 8(2) and in accordance with the law.

If proper implementation of Articles 10 and 11(1) is crucial to the achievement of the Directive's objectives, then in order to assess the adequacy of national provisions pursuant to the Directive, it is necessary:

1. to determine what powers are granted to Member States to exempt data controllers from the duty to provide Articles 10 and 11(1) information to the data subject; and
2. to assess the adequacy of safeguards put in place to accompany any exemptions from this duty.

In this paper, I argue that (unless Article 13 of the Directive is appealed to), in order to implement Article 10, an unqualified duty must be placed on data controllers. Article 10 does not, however, explicitly differentiate cases where data are currently being obtained from the data subject and cases where data were previously obtained from the data subject and the data controller now wishes to make disclosures or process for purposes that were not envisaged at the time of obtaining.[4] Now, if Article 10 covers *all* cases where data are being, or were, collected from the data subject, this implies that it will be necessary for the data controller to go back to the data subject to provide the data subject with information if processing that was not anticipated at the time of collection is to be permitted (unless an exemption is provided via Article 13). On the other hand, if Article 10 only covers cases where data are being collected from the data subject, then unanticipated future processing by a data controller who obtains personal data from the data subject might seem not to be covered by the Directive (with the implication that Member States may regulate this as they wish). I suggest, however, that the possible 'missing case' is covered by Recitals 39 and 40, which suggests a duty in relation to unanticipated processing where data were obtained from the data subject that is conditional in the same way as cases falling under Article 11(1) (where data were not obtained from the data subject by the data controller). Consequently, I argue while Member States may treat all cases where data are/were collected from the data subject under Article 10, the best interpretation requires 'the missing case' to be dealt with in terms of Recitals 39 and 40. I argue, too, that if Article 13 is appealed to modify this picture then reference to Article 13 (or the conditions it refers to) must be made explicitly in legislation, because Article 28(4) requires Member States to empower anyone to hear claims for checks on the lawfulness of processing that is pursuant to the use of Article 13 to restrict the provisions of Articles 10 and 11(1).

As concerns the issue of adequate safeguards, I argue, principally, that national implementing measures are to meet the objectives of the Directive, that any processing under legitimate exemptions from the duties prescribed by Article 10 and 11(1) should be treated as processing likely to pose specific risks to the fundamental rights and freedoms of the data subject, and should, hence, be subjected to prior checking by the Supervisory Authority (or an independent Da

---

[4] While Article 11(1) does cover unanticipated disclosures, it only governs cases where data were not obtained from the data subject.

Protection Official acting under the guidance of the Supervisory Authority), in relation to which I make a few suggestions about the criteria that are relevant in such checks.

Finally, to illustrate my analysis, I examine the UK's implementation of the duty to provide information to the data subject under Articles 10 and 11 of the Directive, and draw attention to what I consider to be its inadequacies. I also examine the effect of this in relation to Section 60 of the Health and Social Care Act 2001 and The Health Service (Control of Patient Information) Regulations 2002 made under Section 60, because these have features that are arguably unlawful in relation to Article 10 of the Directive, in particular, a fact which is obscured by the inadequacies of the UK's implementation.

Powers to Exempt from Article 10 and Article 11(1)

According to Article 11(2),

> Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

There is no parallel exemption provided from Article 10. However, Article 13(1) provides that

> Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
> (a) national security;
> (b) defence;
> (c) public security;
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
> (g) the protection of the data subject or of the rights and freedoms of others.

This could possibly apply to medical research. For example, there might be cases where medical research to develop biological weapons or, more plausibly, to defend against them, could be necessary for (a)–(c). Provision (d) could be appealed to in relation to the investigation of fraud in medical research. Medical research is also, arguably, an important economic or financial interest of the Member States. In so far as (c)–(e) apply, (f) applies. And, at least in principle,

medical research could be argued to be something that individuals have a right to that can be placed in the balance with data protection rights of the data subject.

This said, two things must be borne in mind. First, any restrictions must be necessary to safeguard the interests concerned, and this implies that they will generally have to be applied on a case by case basis, in consequence of which it is arguable that they may not be applied to medical research generically. Secondly, Article 28(4) specifies that

> Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

Matters are further complicated by the fact that what situations are covered by Articles 10 and 11(1), respectively, are open to interpretation. Does Article 10 apply to all controllers who have collected personal data from the data subject? Or does Article 10 only apply to controllers at the point at which they are collecting data from the data subject? If the former, then Member States must (unless they restrict Article 10 via appeal to Article 13(1)) provide that a data controller who has collected personal data from the data subject for specified purposes Y without envisaging its use for purposes Z, but subsequently wishes to use the data for Z, must go back to the data subject to inform of this processing, and may not appeal to any disproportionate effort or impossibility in doing so to avoid having to do so, which might seem unreasonable. On the other hand, if the latter, then the case described does not seem to fall under the ambit of either Article 10 or Article 11(1), because everything under Article 11(1) explicitly applies only where the controller did not obtain the data from the data subject.

However, Recitals 38–40 might be of assistance here. Recital 38 states that, in order for processing to be fair,

> the data subject must be in a position to learn of the existence of a processing operation, and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.

Recital 39 then refers to two cases—processing of data that the controller did not collect from the data subject (which is covered by Article 11(1)), and disclosures that were 'not anticipated at the time the data were collected from the data subject' (which is not covered explicitly by either Article 10 or Article 11(1)), and says of both cases that the 'data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party'. However, Recital 40 then specifies that it is not necessary for 'this obligation' to be imposed when conditions apply that are essentially those specified in Article 11(2).

What does 'this obligation' refer to? One possibility is that it refers to the cases covered by both Recital 38 and Recital 39. However, if this is so, then Article 10 should have two parts. There should be an Article 10(1), which specifies the obligation, and an Article 10(2), which provides an exemption from Article 10(1)

with the same content as Article 11(2). That Article 10 does not have this structure is, I believe, conclusive that Recital 40 refers only to Recital 39 (and not to either Recital 38 or to Article 10). On this basis, Article 10 should be taken to apply only at the point at which data are being collected from the data subject, and the missing case of unanticipated disclosures where the data were collected from the data subject is to be dealt with on Article 11(2) lines by a direct appeal to Recitals 39 and 40 as free-standing provisions. It is quite possible that Article 11(1) was meant to convey this; but its heading unambiguously limits the application of Article 11(1) itself to cases where the information was not collected from the data subject.

To this, it might be objected that Recitals do not *in themselves* have any legally binding force,[5] and that they can only have any force in relation to interpreting Articles in a Directive. Since there is no Article that explicitly covers unanticipated disclosures where data were collected from the data subject, Recitals 39 and 40 cannot be appealed to in order to cover the case of unanticipated disclosures where data were collected from the data subject.

However, in response to this, at least two things can be said. First, even if Recitals have no free-standing legally binding force, this does not prevent them from having a persuasive force, meaning by this that, provided that they do not contradict an Article, they *may*, at least, be appealed to in order to cover cases not covered by the Articles. Secondly, since the main purpose of Recitals is to provide reasons for the Articles, on condition, again, that the Recitals do not contradict the Articles, a teleological approach to the interpretation of a Directive surely permits free-standing use of Recitals to be made where the Articles do not cover important scenarios that are covered by the Recitals.[6]

However, whether or not we can make this response turns on how we choose to interpret Article 10. If we say that Article 10 covers all cases where data were collected from the data subject (thus including data controllers who wish to make disclosures that they did not anticipate or envisage at the time of collection), then Article 10 actually contradicts part of Recital 39 read with Recital 40, and we cannot make this response. On the other hand, if we say that Article 10 only applies at the point of data collection, then there is no contradiction when Recital 39 is read with Recital 40, and we can make this response.

I suggest that the latter is at least a possible reading on purely textual considerations. If so, then I suggest that the use of teleological principles that are well established in EC law[7] also suggests that it is the preferable reading. Consequently, I suggest that using Recital 39 read with Recital 40 to cover

---

[5] See *Gunnar Nilsson, Per Olav Hagelgren, Solweig Arrborn, Agriculture* (Case C–162/97), judgment of 19 November 1998, paragraph 54 of the judgment. However, it is arguable that this is restricted to cases where there is a conflict between a Recital and an Article of a Directive.

[6] For a detailed discussion of the ECJ's treatment of Recitals—see Deryck Beyleveld 'Why Recital 26 of Directive 98/44/EC Should be Implemented in National Law' (2000) 4 *Intellectual Property Quarterly* 1–26.

[7] See L. N. Brown and T. Kennedy, *The Court of Justice of the European Communities* (4th edn., London: Sweet and Maxwell, 1994), 316.

unanticipated disclosures where data were obtained from the data subject is at least permissible, and, indeed, the best reading of the Directive.

Even this, however, does not cover the case of processing for unanticipated purposes when data were collected from the data subject. Nevertheless, if it is permissible to provide an Article 11(2) type exemption for unanticipated disclosures where data were collected from the data subject by appealing to Recital 39 read with Recital 40, then it is surely also permissible to provide such an exemption for processing for unanticipated purposes when data were collected from the data subject.

Finally, it should be noted that both Article 10 and Article 11(1) have an internal restriction to the effect that the additional information referred to in Articles 10(c) and 11(1)(c) need only be provided in so far as necessary to guarantee fair processing. This implies that there might be circumstances in which the provision of such additional information might not be necessary for fairness (and, hence, not obligatory). Consequently, it is open to Member States to make the provision of this additional information in Article 10 subject to proportionality, or practicability, or an equivalent condition. However, it must not be overlooked that this qualification applies only to the additional information of Articles 10(c) (and 11(1)(c)) and not to the information required to be provided by Articles 10(a) and 10(b) (and 11(1)(a) and 11(1)(b)).

The Question of Adequate Safeguards

If there is to be exemption from Article 11(1), then Article 11(2) specifies that Member States must provide appropriate safeguards. The Directive does not, however, specify explicitly or directly what the nature of appropriate safeguards might be. Does this mean that it is entirely at the discretion of the Member States to determine what constitutes appropriate safeguards; or can we infer at least some requirements from the Directive as a whole on the basis of which interpretations of individual Member States could, in principle, be held to be untenable?

The objective of the Directive must constitute the focal point for any specification of appropriate or adequate safeguards. Since the objective of the Directive is to protect fundamental rights and freedoms, in particular privacy, appropriate safeguards must be appropriate measures to protect against breaches of these rights and freedoms. According to standard human rights thinking, in order for there to be a justification for interference with a right, the interference must be necessary for an overriding value, must not be more extensive than necessary, and must be sanctioned by law. In relation to this, appropriate safeguards must be appropriate measures designed to ensure that these conditions are satisfied.

While the Directive does not specify such measures in relation to Article 11(2), it is fairly expansive in relation to exemptions from the duty to notify the Supervisory Authority. When notification is required under Article 18, Article 19(1) requires Member States to provide that the data controller must provide the Supervisory Authority with at least:

(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the processing;
(c) a description of the category or categories of data subject and of the data or categories of data relating to them;
(d) the recipients or categories of recipient to whom the data might be disclosed;
(e) proposed transfers of data to third countries;
(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

This is not dissimilar to the information required to be given to the data subject under Articles 10 and 11(1). Consequently, measures that permit exemption from, or simplification of, notification are, arguably, highly relevant to measures that should accompany exemptions from any duty to inform the data subject.

Unless processing is for the sole purpose of a public register (see Article 18(3)) or for purposes of a political, philosophical, religious or trade union foundation (as specified in Article 8(2)(d)), Article 18(1) requires Member States to provide that wholly or partly automated processing be notified to the Supervisory Authority before it is carried out. Article 18(2) then provides that there may be exemption from, or simplification of, notification

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they [data controllers] specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
  - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive,
  - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

I suggest that these provisions should be treated as a model for appropriate safeguards under Article 11(2). Just as Article 18(2) envisages a Personal Data Protection Official standing *in lieu* of the Supervisory Authority to permit exemption from, or simplification of, notification, so the Supervisory Authority (directly) or a Personal Data Protection Official (indirectly) should be viewed as standing *in lieu* of the data subject whenever there is an exemption from the duty to inform the data subject under Article 11(2) (as well as in cases where data were collected from the data subject—to the extent that this is permissible). This is because not to inform the data subject seriously impairs the data subject's ability to exercise the specific rights (to access, objection, etc.) granted by the Directive, which exists to protect fundamental rights and freedoms, and in particular privacy, in consequence of which, not to inform the data subject constitutes a specific risk

to these rights and freedoms by the very nature of the case. In effect, the notification provisions should apply *whenever* a Member State avails itself of Article 11(2). There is no difficulty with this; for, although notification is only required for wholly or partly automated processing, Article 18(5) provides that:

> Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Alternatively, if notification is not to be required then, at the very least, Article 21(3) should be invoked, which requires that Member States must provide that the Article 19(1) notification information (apart from security information of Article 19(1)(f)) must be given to anyone on request for any data not subject to notification).[8]

This suggests a link to the Directive's provision on prior checking. Article 20 requires Members States to ensure that the Supervisory Authority (or an independent Personal Data Protection Official acting in consultation with the Supervisory Authority) conducts a prior check in relation to processing that represents specific risks to the rights and freedoms of data subjects. While it is up to Member States to determine what processing poses these risks, any exemption from the duty to provide information to the data subject surely poses such a risk. Indeed, as I have already suggested, at least in relation to sensitive data, because lack of this information precludes consent, it arguably automatically involves an interference with the right provided by Article 8(1) ECHR, which requires a justification in terms of Article 8(2) ECHR. While disproportionate effort, as referred to in Article 11(2), is relevant to any such justification, it is surely not appropriate for the data controller to make judgements about this in what is the data controller's own cause. Furthermore, I do not consider it adequate to leave it to the Courts to decide the matter when the data subject makes a complaint. Unless there is prior checking, it is possible, indeed likely, that the data subject will not find out. And, even if the data subject finds out, at least in the case of patients and medical research subjects, he or she is in an inherently vulnerable position in relation to those against whom he or she wishes to complain (as well as generally lacking adequate resources to pursue legal actions).

While the judgements made in prior checks need to be made on a case by case basis, it is possible to suggest a number of things about such checks.

First, it is arguable that it is too onerous to require all exemptions from the duty to provide information to the data subject to be subjected to prior checks. However, even if this is so, it does not follow that prior checks should never be required when this exemption applies, and I suggest that they should at least be carried out where the processing touches on matters of religious, moral or general public sensitivity, simply because these are the cases in which persons are likely to have strong and predictable objections.

---

[8] It should be noted, however, that this is subject to restriction via Article 13, which the requirement to notify the Supervisory Authority is not.

Secondly, specific attention must be given to the security arrangements of Article 17 (which are not subject to exemption) when deciding on a justification for exemption from the provision of information.

Thirdly, if processing does not need to be carried out in personal form then any personal data that is to be processed without informing the data subject should be rendered anonymous or at least securely coded. While this, in my opinion, does not preclude a breach of privacy when the data are used for purposes to which the data subject would object,[9] it is nonetheless necessary to limit the breach if it is otherwise held to be justified.

As regards Article 13, Article 28(4) (which requires Member States to provide for the Supervisory Authority to hear claims for checks on the lawfulness of processing whenever exemptions created with reference to Article 13 are applied) provides a safeguard (though not, in my opinion, one that is as adequate as obligatory prior checking would provide). Apart from this, however, the Article 28(4) provision suggests that Article 13 (or the grounds it provides) must be explicitly referred to when Article 13 is used to restrict the application of Articles 10 and 11(1) (or the other Articles it may be used to restrict). This surely suggests that Article 13 should not be something that a Member State can claim in justification when its provisions on Articles 10 and 11(1) are challenged, if this basis has not been claimed in the implementing law. For, unless this basis is claimed it will not be possible for persons to identify what processing they may refer to the Supervisory Authority's attention in relation to Article 28(4).[10]

---

[9] See Deryck Beyleveld and David Townend 'When is Personal Data Rendered Anonymous? Interpreting Recital 26 of Directive 95/46/EC' (2004) 6 *Medical Law International* 2: 73–86.

[10] It should be noted that exempting from the duty to provide information *generally* will, in effect, remove the right to object under Articles 14(a) and 14(b). Since neither Article 13 nor Article 11(2) provides any derogation from Article 14(b), it is probably better for implementing laws to treat the information provision required by the latter separately from that required under Articles 10 and 11(1).

In addition, it should be noted that Article 14(a) specifies that the conditions under Article 7(e) and (f) for removing the prohibition on processing of personal data (processing in the public interest and processing for legitimate purposes of the data controller) may not be deployed without granting the data subject the right to object on compelling legitimate grounds relating to his/her particular situation unless national legislation removes this right. This appears to have the consequence that, whenever there is exemption from Articles 10 or 11(1), the conditions referred to in Articles 7(e) or (f) may not be appealed to in order to legitimate processing, unless the right to object of Article 14(a) is removed for these cases under national legislation. I suggest, further, on the basis of requirements of transparency, that such implementing law under Article 14(a) may not be taken to be implicit in any domestic provisions implementing Article 11(2).

The UK's Implementation of Articles 10 and 11

If the above analysis is correct, then there are essentially three legitimate strategies that Member States can adopt when implementing Articles 10 and 11.

a. They may implement Articles 10 and 11 without any exemptions based on Article 13, or by reference to Recitals 39 and 40. If so, they will require Article 10 information to be given to the data subject whenever a data controller who obtained personal data from the data subject intends to process the data for unanticipated purposes, or to make unanticipated disclosures.
b. They may appeal to Recitals 39 and 40 to create an exemption along the lines of Article 11(2), thereby not requiring a data controller, who obtained personal data from the data subject to provide Article 10 information to the data subject in relation to processing for unanticipated purposes, or the making of unanticipated disclosures if the provision of information would be impossible, involve disproportionate effort, etc.
c. They may create exemptions from the provision of information to the data subject on the grounds provided by Article 13 (whether or not they have appealed to Recitals 39 and 40 to cover the 'missing case' of processing for unanticipated purposes or the making of unanticipated disclosures where the data controller has obtained the personal data from the data subject).

Which of these basic strategies has been adopted by the Member States (and those of the New Member States or NAS that have passed legislation with reference to the Directive) (as well as any other approaches) is beyond the scope of this paper. Here, I will pay detailed attention only to the UK's implementation, the main purpose of which is to illustrate my general analysis of Articles 10 and 11(1).

The UK's Data Protection Act 1998 (DPA) implements Articles 10 and 11 in Schedule 1 paragraphs 2 and 3. There are at least three features of this implementation that merit comment.

First, where data are obtained from the data subject (the Article 10 case), the data controller has a duty to ensure 'so far as practicable that the data subject has, is provided with, or has made readily available to him, the information' (Schedule 1 Part II Paragraph 2(1)(a)). Article 10 does not, however, make this duty subject to practicability, quite probably because it does not recognize the possibility of impracticability in this case. Of course, Article 10 does specify that 'further information' need only be given in so far as this is, taking the specific circumstances into account, necessary for fairness. If 'practicability' refers to this then it is legitimate. However, it must be noted that (in Article 10) this qualification does not apply to the basic information concerning the identity of the controller and the purposes of the processing that are intended, but only to 'further information'. Alternatively, the introduction of a condition of practicability might be interpreted as meaning that information about purposes of processing and disclosures need only be given in so far as these are envisaged or reasonably anticipated. If so, then according to my reading of Recitals 39 and 40, this would

be legitimate. It is also legitimate if 'practicability' is intended to qualify the amount and detail of information (about purposes of processing, in particular) that must be provided, rather than as a condition qualifying the duty to provide information at all. However, as the relevant paragraph is worded, it gives no direction about what interpretations are intended[11] (and, see below, it is arguable that an illegitimate interpretation is required to square some provisions of The Health Service (Control of Patient Information) Regulations 2002 with the Directive).

Secondly, the information that must be given is less specific than indicated in the Directive, being information about

> (a) the identity of the data controller,
> (b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
> (c) the purpose or purposes for which the data are intended to be processed, and
> (d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair. (Schedule 1 Part II Paragraph 2(3))

While there is nothing improper about this, it is less than helpful not to have included the examples of such further information that the Directive provides.

Thirdly, whereas (where the data were not obtained from the data subject) Article 11(2) of the Directive does not require the information to be provided if this proves impossible, Schedule 1 Part II Paragraph 2(1)(b) states (as Paragraph 2(1)(a) states for the Article 10 case) that the information need only be provided so far as is practicable. Of course, 'impracticable' could be interpreted to mean 'impossible'. It is, however, capable of being given weaker interpretations and quite probably will be.

Part IV of the DPA (Sections 27 to 39) provides general exemptions, some of which are exemptions or powers to exempt from the duty to provide information to the data subject.[12] Many of these exemptions are clearly made, at least implicitly, by reference either to Article 3(2) (which places processing for purely domestic

---

[11] Although the Information Commissioner does not consider this matter explicitly in *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998), paragraph 3.1.7.3, 33, the guidance focuses on the quality of the information provided and suggests that the only exemptions from the duty to provide information to the data subject are provided under Part IV of the Act (see below).

[12] Many of the sections give the Secretary of State the power to make regulations. This power has been used in several cases.

In Part IV, the duties implementing Articles 10 and 11 are not identified separately but as part of what is termed 'the subject information provisions' (which also include the subject access provisions of Section 7 that implement part of Article 12), or 'the non-disclosure provisions', which also include the 2nd, 3rd, 4th and 5th data protection principles (cf. Articles 6(1)(b)–(e)), the right to object of Section 10 (cf. Article 14(a)) and the right to rectification, blocking and erasure of Section 14(1)–(c) (cf. part of Article 12) to the extent that these are incompatible with the disclosure in question.

purposes as well as activities beyond the scope of EC law outside of the scope of the Directive) (see Section 36), Article 9 (which permits processing that is solely for journalistic, artistic or literary purposes to be exempted from the data protection principles, though only to the extent that this is necessary to reconcile the right to privacy with the right to freedom of expression) (see Section 32),[13] or Article 13 (which, to an extent, overlaps with Article 3(2)). In relation to Article 13, there are exemptions from the duty to provide information in relation to national security (Section 28), the prevention and detection of crime (Section 29), and various regulatory activities (Section 31). Section 38 empowers the Secretary of State to pass regulations exempting from the duty to provide information in the interests of the data subject, or for protection of the rights and freedoms of others. The basis for some of the other exemptions is less clear: e.g., the powers under Section 30 (to exempt from the subject information provisions in relation to health, education and social work data), Section 34 (in relation to information made public by or under an enactment) and Section 35 (when disclosure is required by law or in connection with legal proceedings). Evaluation of the situation is not helped by the fact that, in Part IV, the provisions implementing Articles 10 and 11 are not identified separately (see footnote 12). This is unfortunate, because some of the exemptions, e.g. that under Section 30, are easier to relate to these conjoined provisions than to those implementing Articles 10 and 11 (and I do not find it surprising that the Regulations that have been made to date under Section 30 concern only Section 7 of the DPA (which concerns subject access) (see Statutory Instruments 413–416, 2000).

Despite what has been said in relation to the DPA's implementation of Articles 10 and 11, it is arguable that the departures from Articles 10 and 11 that the implementation appears to involve are to be justified as use of a Member State's discretion under Article 13. However, no provision is made in the DPA for the Supervisory Authority to hear claims for checks on the lawfulness of provisions pursuant to Article 13 by anyone (as required by Article 28(4)). This is significant enough in relation to the general exemption powers of Part IV of the DPA. However, it might, not unreasonably, be thought that such provision need only be made when these powers are exercised in regulations passed under the relevant Sections. But, at the same time, such a thought reinforces the perception that the provisions of Schedule 1 Part II paragraphs 2 and 3 (which, as they stand, make no reference to Article 13, or any of the justifications for restriction of the Directive provisions that it provides) cannot legitimately rely on Article 13, unless, and until sector-specific regulations are passed under Part IV.

Finally, as regards appropriate safeguards, while the UK does make provision for prior checks of processing likely to present specific risks to fundamental rights and freedoms, it has done so only on condition that the Secretary of State passes regulations specifying 'assessable processing' (see Section 22). However, no such regulations have yet been passed and there is no indication that processing that

---

[13] The exemption of Section 32 is, arguably, too wide in relation to the Directive. However since this exemption has little application in relation to medical research, I will not pursue the matter.

enjoys an exemption from the requirements of Articles 10 and 11(1) will be considered assessable processing.[14] As safeguards, the Secretary of State has specified in the Data Protection (Conditions Under Paragraph 3 of Part II of Schedule 1) Order 2000 (Statutory Instrument No. 185) that, whenever there is exemption from the duty to provide information to the data subject, the data controller must give the information to anyone who requests it, and that data controllers must keep a record of reasons for considering that disproportionate effort would be involved in providing the data subject with the information. This approach is reactive rather than proactive and surely insufficient.

While the Health and Social Care Act 2001 (HSCA) is independent of the DPA, Section 60 of the HSCA raises issues to which the UK's implementation of Articles 10 and 11 of the Directive are relevant.

Section 60 of the HSCA gives the Secretary of State the power to pass regulations (which must be approved by both Houses of Parliament, the so-called 'affirmative procedure') that render it lawful to process personal data without the subject's consent despite any obligation of confidence that is owed to the patient. The following conditions must be satisfied:

a. The regulations must be in the interests of improving patient health care or in the public interest (s. 60(1)).
b. It must not be reasonably practicable to obtain consent, because the regulations:

> may not make provision requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such regulations, having regard to the cost of and the technology available for achieving that purpose (s.60(3)).

Section 60(2)(c) provides that:

> where prescribed patient information is processed by a person in accordance with the regulations, anything done by him/her in so processing the information shall be taken to be lawfully done despite any obligation of confidence owed by him in respect of it.

Section 60(6) then goes on to say,

> Without prejudice to the operation of provisions made under subsection (4)(c),[15] regulations under this Section may not make provision for, or in connection with the processing of prescribed patient information in a manner inconsistent with any provision made by, or under the Data Protection Act 1998 (c. 29).

---

[14] One might, perhaps more accurately, say that the DPA does not provide for prior checking but only provides for provision for prior checking to be made.

[15] Quite clearly subsection (2)(c) is meant. What is subsection (2)(c) in the Act was subsection (4)(c) in earlier drafts. However two subsections (what were subsections 1 and 2) were dropped at the last moment; but hasty editing has not picked up on this. Similarly the Act at various places makes reference to subsection (3) when it means subsection (1).

Section 60(2)(c) is ambiguous. It can be interpreted as stating that regulations passed under Section 60 render processing not unlawful *on account of being a breach of confidence* (but do not necessarily render processing lawful, as there might be reasons other than breach of confidence why processing might be unlawful). Alternatively, it can be interpreted as stating that regulations will render processing of confidential patient information lawful.

The interpretation given is important, because, under the first reading, Section 60(2)(c) says little more than that, once regulations are passed, processing of regulated data will not be a breach of the first data protection principle of the DPA (that data must be processed fairly and lawfully, etc.) *on account of being in breach of confidence*, implying that processing that is contrary to the DPA for any other reason will still be unlawful. However, under the second reading, Section 60(2)(c) appears to claim that processing of regulated data cannot be unlawful on account of breaching any provisions of the DPA.

The second reading is surely not legitimate (though I expect that is the way medical researchers will be tempted to read it). Since the DPA is meant to implement the Data Protection Directive, a claim that the DPA cannot render processing that falls under the regulations unlawful is tantamount to the claim that the Directive cannot render them unlawful, and this is contrary to the doctrine of the supremacy of EC law. However, I imagine that it might be claimed that this is of theoretical significance only, on the grounds that the conditions that must be satisfied for regulations to be passed under Section 60 are sufficient to render processing lawful under the DPA (and, by implication, the Directive).

Let us assess such a claim. To be lawful under the DPA (considering only its first data protection principle), processing of personal data on a person's health must satisfy at least one condition from Schedule 2 of the DPA (cf. Article 7 of the Directive), at least one condition from Schedule 3 (cf. Article 8 of the Directive), conditions of fair processing laid down in Schedule 1 Part II (which include the Act's implementation of Articles 10 and 11), and any other conditions of fair and lawful processing that are applicable under UK law (such as the common law on confidentiality). Because the DPA must, if possible, be interpreted in conformity with the rights of the ECHR recognized by the Human Rights Act 1998 (HRA) (see Section 3 of the HRA), it is arguable (see above) that *at least* Schedule 3 conditions other than consent may not be appealed to unless the obtaining of consent is impracticable.[16] Provision for this is, however, made by Section 60 of

---

[16] This is not the view taken by the UK's Information Commissioner in *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998) paragraph 3.15, 30, where it is stated that: 'All the conditions provide an equally valid basis for processing. Merely because consent is the first condition to appear in both Schedules 2 and 3, does not mean that data controllers should consider consent first'.

However, at least where the data controller is carrying out public functions (which doctors in the NHS do), the Commissioner appreciates that the HRA applies and that it would be unlawful to use private sensitive data without consent unless there is an overriding justification for doing so (see paragraph 3.14, 30). This does not sit easily with the view given at 3.15. Perhaps, the Commissioner takes the view that the other conditions provide

the HSCA. Equally, Section 60 is in line with the requirements of justifying a breach of the right to privacy of Article 8(1) ECHR under Article 8(2) ECHR when it specifies that the regulations must be made in the interests of healthcare, or the public interest. Then, as far as fair processing is concerned, Section 60 arguably satisfies Schedule 1 Part II paragraph 2 of the DPA (cf. Articles 10 and 11(1) of the Directive), because this does not require information to be given to the data subject in so far as it is not practicable to do so (and it is arguable that if consent is not practicable then provision of information to the data subject is also not practicable).

However, this latter point raises the question of the adequacy of the UK's implementation of Article 10 of the Directive, in particular; for (as I have already pointed out), Article 10 does not make provision of information to the data subject conditional on 'practicability', and while Article 13 gives Member States the power to restrict Article 10 in such a way, the UK has not explicitly appealed to Article 13 for this purpose, and an explicit appeal seems to be necessary if Article 28(4) is to be satisfied.

Furthermore, it must not be forgotten that Article 14(a) specifically does not permit public interest aims to render processing legitimate unless the data subject is given the opportunity to object, unless this right is removed by legislation. The DPA has not done so explicitly. Indeed, in removing the right to object in relation to a number of other conditions of Article 7, but not in relation to the claim to the public interest (see Section 10 of the DPA), the UK would seem to have retained the right to object in relation to public interest justifications for processing without consent.

Then, if Section 60 of the HSCA itself can be questioned, so too can The Health Service (Control of Patient Information) Regulations 2002,[17] that has been passed with reference to the HSCA. While there are numerous difficulties with interpretation of these provisions, and the provisions are important for the second phase of the PRIVIREAL project in relation to the statutory role they create for research ethics committees, I shall not consider these here, as this would take us too far from issues specific to Articles 10 and 11 of the Directive. However, in relation to the latter, it should be noted that Regulation 2, *inter alia,* permits personal data on cancer patients to be recorded on cancer registries without the consent of the patients. By implication, this permits the data to be recorded without even informing the patients, because in order to satisfy Section 60 of the HSCA it must be reasonably impracticable to obtain consent for the regulation to be valid, and it is surely impracticable to obtain consent only if it is impracticable to inform the patient. However, the Regulations do not discriminate between the clear Article 10 case where data are being obtained from the data subject, the less clear Article 10 case (where data were obtained from the data subject but the controller now

---

justifications in these terms. I disagree, because for an Article 8(2) ECHR justification to apply it must be necessary to interfere with the right provided by Article 8(1), and it will not be necessary if consent can be obtained (and will not in itself threaten more important rights).

[17] Statutory Instrument 2002, No. 1438.

wishes to use it for an unanticipated purpose, which I have argued is covered by Recitals 39 and 40) and those cases that fall under Article 11. Thus, the Regulations can only be acceptable under the HSCA (let alone the Directive) if it is true that it is impracticable to get patients' consent for their data to be entered on cancer registries when the doctor is in the process of getting this data from the patient.

Related to this, it should be noted that Section 60 of the HSCA is supposed to be an interim measure until means of respecting confidentiality consistent with the public interest/interests of health care can be developed (which is reflected in Section 60(4), which provides that the Secretary of State must review the provisions annually). However, if it is considered impracticable to get consent from patients who are in front of the doctor, then it is exceedingly difficult to see what measures could possibly be produced to render regulations unnecessary.

In order to put all of this in proper perspective, it is necessary to appreciate that Section 60 of the HSCA is the result of a concerted campaign by epidemiologists, who have pressed for all medical research to be exempted altogether from the DPA.[18] The thrust of the arguments presented, which focused on cancer research, was that it is impracticable to get consent from patients for the entry of their personal data on cancer registries and for the use of this in medical research and because the patients' clinicians would not always co-operate, resulting in less than 100 per cent of cases being entered on cancer registries, which would seriously compromise the value of the data. The fact that such arguments were accepted by Parliament, is, in my opinion, nothing short of scandalous. In approving Regulation 2 of The Control of Patient Information Regulations, Parliament either accepted the ridiculous view that doctor's reluctance to ask their patients for consent (or to give them the opportunity to object, which is more directly relevant to the issues raised by Articles 10 and 11 of the Directive) renders the getting of consent impracticable, or the view that it is in the public interest not to obtain consent (or to give the opportunity to object) because the fact that some patients might not consent (or might object) would seriously compromise the quality of data on cancer registries. However, in relation to the second possibility there is no reason to believe that more than a small percentage would refuse to give consent or object, there is no reason to assume that consent is related to the clinical condition in question, and a 100 per cent sample is, in any event, impossible as, for cancer generally, 100 per cent must mean 100 per cent of the human race.

Concluding Remarks

In this paper I have presented a very personal view, which many will no doubt find controversial. What centrally guides my analysis is the conviction that the

---

[18] See 'Cancer experts call for action on GMC's confidentiality rules' (2 November 2000) *Health Service Journal*. 4.

Directive must be interpreted and applied by attention to its objectives, remembering that according to Article 249 EC (ex Article 189), Directives are binding on Member States in relation to the 'result to be achieved'. Since, in this case, the result to be achieved includes the protection of fundamental rights and freedoms (albeit, because of the competence of the EC to legislate, only as means to the free-flow of personal data between the Member Sates) my analysis is guided by considerations of principle that are always implicated whenever attention to fundamental rights and freedoms is central. While others may have different views on what the implications of protection of fundamental rights and freedoms are, it is not debatable that such a focus must be central. It should also be obvious that the duty to provide information to the data subject of Articles 10 and 11(1) is vital if data subjects are to be able to exercise their fundamental rights and freedoms. Indeed, I do not believe it to be a distortion to say that these two Articles are the lynchpin of the whole Directive, in that any failure to implement these provisions adequately will fundamentally undermine the objectives of the Directive. Whether or not the partners in the PRIVIREAL Project are capable of reaching a consensus about the issues raised in this paper, the issues raised in it are, consequently of the first importance in relation to any assessment of whether the Member States have adequately implemented the Directive (and *a fortiori,* will be of equal importance later in the PRIVIREAL Project in relation to any recommendations that the Project will wish to make to the European Commission).